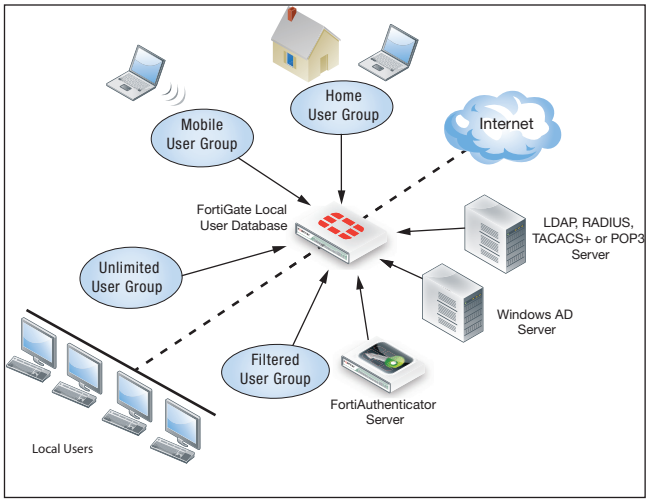
Authentication

FortiOS authentication identifies users and, based on identity, allows or denies network access while applying any required additional security measures.

Authentication in FortiOS

Authentication is an important part of your network security, as it allows you to identify network users, ensuring that your network is only accessed by authorized users, and allowing different users to have access to different data and services. FortiOS authentication controls access to various resources for wired and wireless networks, as well as being used for both IPsec and SSL VPNs.



FortiOS authentication integrates with the following technologies:

- Windows AD and other domain services using Single Sign-On (SSO)
- LDAP, RADIUS, TACACS+, and POP3 servers
- FortiAuthenticator units
- Certificates
- FortiToken, FortiToken Mobile, and third-party two-factor authentication technologies, such as RSA SecurID

FortiOS user authentication is based on user definitions and user groups, which are added to identity-based security policies, SSL VPN portals, or IPsec VPN configurations. Creating users and user groups determines where to store the user credentials and which authentication method to use.

Single Sign-On (SSO)

Single Sign-On (SSO) allows logged in users to access resources through the FortiGate unit without being asked again for their credentials. There are several ways in which FortiOS supports SSO:

- Fortinet Single Sign-On (FSSO) provides single sign-on capabilities to Windows AD, Citrix, or Novell eDirectory users with the help of agent software installed on these networks. In a Windows AD network, FSSO can also provide NTLAN Manager (NTLM) authentication service to the FortiGate unit.
- FortiOS can provide SSO capability for Windows AD networks without agent software by directly polling the Windows AD domain controllers.

- RADIUS Single Sign-On (RSSO) allows FortiOS to authenticate users transparently if they have already authenticated on a RADIUS server.
- FortiOS can integrate with a FortiAuthenticator server to provide SSO authentication.

Authentication challenge

Authentication challenges require a user to enter their credentials to access network resources through the FortiGate unit, regardless of whether they have already been authenticated on the network. FortiOS supports the following types of authentication challenges: password authentication, certificate authentication, and two-factor authentication. Authentication occurs using HTTP, HTTPS, or FTP. FortiOS can also redirect HTTP authentication challenges to a secure HTTPS channel.

The types of connections that typically require an authentication challenge include:

- Identity-based security policies
- IPsec VPNs
- SSL VPNs
- Any connections involving specific FortiGate features, such as web filter overrides or access to administrative functions

FortiOS authentication challenges apply to wireless and wired networks in the same way, as authentication for both network types is applied in the security policy that controls the network traffic.

Identity-based security policies

Identity-based security policies are required for FortiOS to distinguish between different groups of users and to implement access levels simply according to the user's identity. These security policies contain authentication rules that match users or user groups with access privileges.

When an identity-based security policy is used, any user attempting to connect through a FortiGate unit must be authenticated before they are allowed access. Once the user credentials have been entered, FortiOS searches for an authentication rule in the policy that matches the user's identity.

If the user's credentials are accepted, the authentication rule is used to determine the following: available services (HTTP, FTP, etc.), access schedule, security features, traffic shaping, logging, and whether or not the user must read and accept a customizable network usage policy or disclaimer.

IPsec VPN

FortiOS supports several methods to authenticate IPsec VPN users:

- **Preshared keys:** remote users must obtain the preshared key for an IPsec VPN, which they then enter into their VPN client configuration. When the client attempts to connect, FortiOS checks the key to make sure it matches. If the keys do not match, the VPN tunnel is not established.
- **RSA certificates:** certificates are used in a similar manner to preshared keys. FortiOS checks to make sure that the correct certificate is being used during a connection attempt and will refuse the connection if the certificate does not match.
- **Extended authentication (XAUTH):** after authentication by preshared key or certificate, remote users enter a username and password to connect to the VPN. Only users who belong to the user group specified in the XAUTH configuration are allowed access. IPsec users authenticated from a RADIUS server can also have their IPsec tunnel virtual IP address assigned from their RADIUS record.

SSL VPN

FortiOS supports the creation of multiple SSL VPN portals, each providing access to a unique combination of network resources and services. Different user groups can be added to each portal and only members of the user groups added to a given portal have access to the services provided by that portal.

When an SSL VPN user logs in, their credentials are matched with a user group and the user is allowed access only to the portal that includes their user group. SSL VPN users authenticated from a RADIUS server can have their SSL VPN virtual IP address assigned by FortiOS from IP information recorded in the RADIUS record.

Local user database

User accounts can be stored directly on the FortiGate unit, to manage user credentials without relying on other resources. This information is only used to authenticate users connecting to that specific FortiGate unit.

External authentication servers

FortiGate units can integrate with the following types of external servers: LDAP, RADIUS, TACACS+, and POP3.

If multiple servers are used, they can be ranked as primary, secondary, or tertiary. This way, the secondary server will only be contacted if the primary is unreachable, while the tertiary server is only contacted if the primary and secondary servers are both unreachable.

LDAP

Lightweight Directory Access Protocol (LDAP) servers provide organization-wide access to member credentials. FortiOS can integrate with multiple LDAP servers and can support any LDAP server port, common name identifier, distinguished name, and one of three bind types: simple, anonymous, and regular. Communication with the LDAP server can be unencrypted or can use LDAP over SSL (LDAPS) certificates or STAR TTLS protocol for secure communications.

RADIUS

Remote Authentication Dial In User Service (RADIUS) servers provide authentication, accounting, billing, and user tracking. FortiOS can integrate with multiple RADIUS servers each with its own RADIUS port, primary and secondary server IP address, and server secret key. FortiOS supports PAP, CHAP, and MS-CHAP v1 and v2 authentication schemes. Also supported are various RADIUS attributes such as Microsoft Vendor-specific attributes (NAS IP/Called Station ID), the Framed-IP-Address attribute for assigning SSL VPN client IP addresses, Acct-Input-* / Acct-Output-* attributes for accounting, and H3C compatibility, which allows authentication to be supported with two RADIUS attributes. Wireless devices can also be authenticated based on their MAC address.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) servers provide similar functionality to RADIUS servers, but TACACS+ separates authentication and authorization into two operations and uses TCP for communication rather than UDP. FortiOS supports TACACS+ authentication using ASCII, PAP, CHAP, or MSCHAP and can integrate with multiple TACACS+ servers.

POP3

Firewall authentication can also authenticate users using the email accounts stored on a Post Office Protocol 3 (POP3) server. The POP3 server functions like any external authentication server.

FortiAuthenticator

FortiAuthenticator is an user identity management solution that delivers authentication via RADIUS server and LDAP, secured by strong two-factor authentication methods for multiple FortiGate and third-party devices. FortiAuthenticator provides central management of users, integration with third party LDAP/AD, and management of FortiTokens, together with user self-registration and password reset. The RADIUS server delivers 802.1X EAP (PEAP, TLS, TTLS) for wired and wireless authentication. FortiAuthenticator can also replace the FSSO Collector Agent on a Windows AD network and deliver additional identity detection methods including captive portal, intranet widgets, SSO Mobility Agent, and RADIUS Accounting.

Certificate-based authentication

An RSA X.509 server certificate is a small file issued by a Certificate Authority (CA) that is installed on a computer or FortiGate unit to authenticate itself to other devices on the network. When one party on a network presents the certificate as authentication, the other party can validate that the certificate was issued by the CA.

Certificates provide the authentication basis for SSL-based secure communications, such as SSL VPN and HTTPS and can also provide peer authentication for IPsec VPNs. Certificates are stored in the FortiOS certificates database, into which both CA and server certificates can be imported.

FortiOS also supports creating a certificate signing request (CSR) for submission to a CA, as well as online submission using SCEP. Certificate revocation lists (CRLs) can also be updated from online servers using HTTP, LDAP, SCEP, or local file import.

Public-key infrastructure (PKI) user accounts can be added to FortiOS to identify the users' certificates by using a text string in a certificate; for example, an email address. The CA certificate must be specified and be available on the FortiGate unit to verify the user's certificate. A special type of user group can be created, which contains PKI users. An IPsec VPN can be configured to allow access to any member of the specified user group who has a valid certificate.

Two-factor authentication

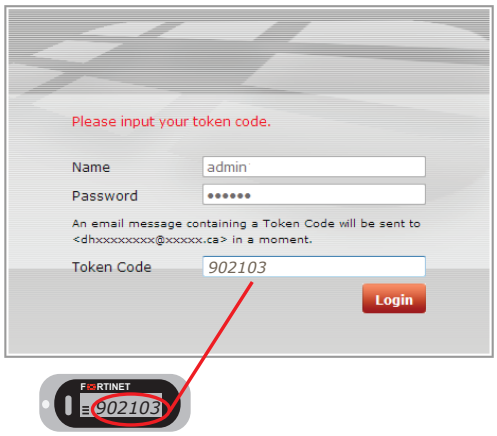
Two-factor authentication, which can be used for connections to both identity-based policies and VPNs, requires a user to provide an additional means of authentication. In addition to their credentials, users must provide either a certificate that is installed on the user's computer, or a randomly generated multi-digit number, often called a token. Users can receive tokens using a one-time password (OTP) system or by having it sent to them via email or SMS text messaging.

FortiToken and FortiToken Mobile

FortiToken generates a unique, time-based token used in two-factor authentication. There are two types of tokens: hard tokens, which require the use of FortiToken hardware, or soft tokens, which are created using the FortiToken Mobile application, available for Android and iOS.

The serial number for FortiToken hardware units must be registered on the FortiGate unit and verified with ortiGuard servers before it can be used. If a token is lost or stolen, an administrator can either disable or delete it to prevent unauthorized use.

FortiToken mobile devices generate tokens using a serial number that can be found on the FortiGate unit. This number can either be entered manually or used to create a QR code. The application is protected by a PIN in case the mobile device is lost or stolen.



When using FortiToken, the login prompt first displays the usual username and password fields. Upon successful entry of that information, an additional field appears for entering the six-digit token.

Captive portal

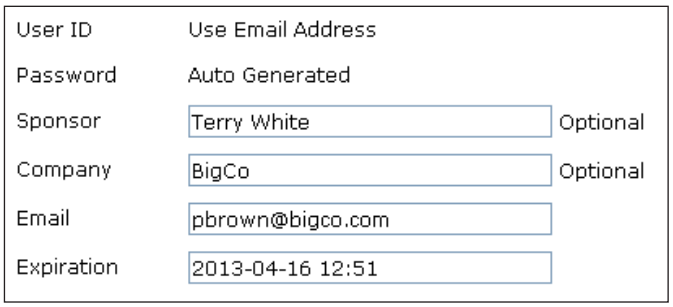
Once a user has entered their credentials to access the Internet, a captive portal can be used to bring them to a web page containing your acceptable use policy or other information. No matter what URL the user initially requested, the portal page is returned. Only after authenticating and agreeing to usage terms can the user access other web resources.

Captive portals can be configured for any interface on the FortiGate, both for wired and wireless connections. Portals can also be hosted on external servers, allowing several FortiGates to use the same portal.

Monitoring users

FortiOS includes the usernames of authenticated users in logs and reports, which can be searched by username. Reports available from FortiOS and FortiAnalyzer can identify the activities of individual users. Banned user quarantine data will also show the usernames of authenticated users, and their quarantine status can be recorded or changed.

Guest accounts



Temporary guest accounts can be created on a FortiGate unit that provide users with credentials to temporarily log onto the network for a set duration. A limit can be set for the maximum number of guest accounts that can be created.

To allow guest accounts to be made, a guest user group must be created. This user group defines how the user ID and password will be created. After this is done, new accounts can easily be generated and a separate admin account can be created solely for the purpose of creating guest accounts, reducing the administrator workload for large events or offices that have frequent visitors requiring temporary Internet or network access.

Authentication-based routing

FortiOS supports authentication-based routing, which associates a user group with one or more routes. This allows all traffic from the user group to be routed to a specified gateway, which can be useful when distinguishing users from different organizations that need to be routed to different Internet gateways.